IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF 2114 WINDSOR AVE APT. # 6, ROANOKE, VIRGINIA 24015 IN THE MATTER OF THE SEARCH OF JOSHUA LEE JENNINGS IN THE MATTER OF THE SEARCH OF A 2014 JEEP, VIRGINIA REGISTRATION TVD-4223	7-24-mj-28 7-24-mj-29 Case No. 7-24-mj-30 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR SEARCH WARRANTS

I, Brandon Smock, a Special Agent ("SA") with Homeland Security Investigations, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for search warrants to search the following for contraband, along with evidence and instrumentalities of violations of Title 18, U.S. Code, Section 2252, as more specifically described in Attachment B of this affidavit:

   a. The premises at **2114 Windsor Ave Apt. # 6, Roanoke, Virginia 24015** ("SUBJECT PREMISES"), located in the Western District of Virginia, and as further described in Attachment A-1;

   b. The person of **Joshua Lee JENNINGS**, Date of Birth 10/XX/1981 ("SUBJECT PERSON") along with any containers such as bags or boxes within his immediate control as further described in Attachment A-2; and

c. A blue/grey in color Jeep, Virginia Registration: TVD-4223 and Vehicle Identification Number (VIN): 1C4NJCBA2ED881780 ("SUBJECT VEHICLE") as further described in Attachment A-3

2. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been employed by HSI since July 2019. As such, I have attended and graduated the Federal Law Enforcement Training Center Criminal Investigator Training Program as well as the HSI Special Agent training program. Prior to becoming a Special Agent, I was a sworn Police Officer with Prince William County Police Department in Virginia beginning in 2012. In the fall of 2016, I became a Detective assigned to the Special Victims Unit of the Prince William County Police Department Criminal Investigations Division. In that capacity, I investigated various criminal offense, including physical and sexual assault offenses against children. In the fall of 2017, I was assigned to the Northern Virginia/District of Columbia Internet Crimes against Children ("ICAC") Task Force. Shortly after, I was sworn in as a Special Police Officer with the Virginia State Police. I was later sworn in as an HSI Task Force Officer. During my time as a Detective, I became a certified Child Forensic Interviewer and became certified in forensic acquisition of digital evidence, Peer-to-Peer data sharing investigations, and undercover chat concepts and techniques. As a part of my current duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography, including violations involving production, distribution, receipt, transportation, possession and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the area of child pornography and child exploitation and have observed and reviewed child pornography, as defined in 18 U.S.C. § 2256(8), numerous times in connection with my duties. Thus, due to my

training and experience, I am able to identify child pornography when I see it. I have training and experience in the enforcement of the criminal laws of the United States, including the preparation, presentation, and service of subpoenas, affidavits, criminal complaints, search warrants, and arrest warrants. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. I am thus a "federal law enforcement officer" as defined by Fed. R. Crim. P. 41(a)(2)(C).

3. I am familiar with the information contained within this Affidavit based upon the investigation I have conducted to date, which includes information provided by other law enforcement agents; written reports about this and other incidents; information gathered from the service of administrative summons; and my experience, training, and background as a Special Agent. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning the investigation. I have set forth only the facts I believe are necessary to establish probable cause to believe that contraband, along with evidence and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of child pornography) and 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (possession of child pornography) are presently located at the SUBJECT PREMISES.

DEFINITIONS

4. The following definitions apply to this Affidavit and its attachments:

a. Title 18, United States Code, Section 2256(2) defines "sexually explicit conduct" as actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the anus, genitals, or pubic area of any person.

b. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), consists of visual depictions of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

e. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

f. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP

assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

g. "Computer hardware," consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. "Computer passwords and data security devices," consists of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. "File Transfer Protocol" ("FTP"), is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet.

FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

j. "Hash value," is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

5. Based on my training, experience, and research, I know that electronic devices such as cellphones and tablets have capabilities to allow them to act as computers that access the internet and as electronic storage media devices that likely contain evidence and records relevant to this investigation. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN OR VISUAL DEPICTIONS OF CHILDREN

6. Information set forth elsewhere in this Affidavit strongly suggests that the target of this investigation has a sexual interest in children or in sexually explicit images and videos of children. My knowledge of these types of individuals and their characteristics is based on my experience as an HSI agent and the training I have received focused on crimes against children. Based upon such training and experience, as well as upon information provided to me by other law enforcement officers, I am aware of the following general characteristics, which may be exhibited in varying combinations and to varying degrees:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies

they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. They may also use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections can be maintained for several years to enable the individual to view the collection, which is valued highly. On the other hand, my recent experience suggests that due to the accessibility and availability of child pornography on the Internet, some offenders engage in a pattern of viewing or downloading child pornography online and then deleting the material, instead of maintaining collections. Even where offenders delete child pornography, it is frequently possible to recover deleted files using digital forensic tools.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; maintain correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names,

addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f. Individuals whose sexual interest in children or images of children has led them to purchase access to paid websites or other commercial sources of child pornography frequently maintain the financial records of those transactions at their residences.

EXPLANATION OF PEER-TO-PEER FILE SHARING

7. Based on my training and experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know that Peer-to-Peer ("P2P") file sharing is a method of communication available to Internet users through the use of special software programs or clients. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the Internet. There are multiple types of P2P file sharing networks on the Internet. To connect to a particular P2P file sharing network, a user first chooses to download a P2P client software program for a particular P2P file sharing network, which can be downloaded from the Internet.

8. A particular P2P file sharing network may have different P2P client software programs that allow access to that particular P2P file sharing network or multiple P2P file sharing networks. These P2P client software programs share common protocols for network access and file sharing. P2P client software allows user(s) to set up file(s) on a computer to be shared on a

P2P file sharing network with other users on the network. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network. For example, one P2P client program is BitTorrent.

EXPLANATION OF THE BITTORRENT NETWORK

9. The BitTorrent network is a popular and publicly available P2P file sharing network. Most computers that are part of this network are referred to as "peers" or "clients." A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

10. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, qBitTorrent, libTorrent, µTorrent client program, and Vuze client program, among others. These client programs are publicly available and typically free P2P client software programs that can be downloaded from the Internet.

11. During the installation of typical BitTorrent network client programs, various settings configure the host computer to share files via automatic uploading. This is commonly referred to as "passive distribution."

12. As an example, during the downloading and installation of the publicly available µTorrent client program, the license agreement for the software states the following. "Automatic Uploading. µTorrent accelerates downloads by enabling your computer to grab pieces of files from other µTorrent or BitTorrent users simultaneously. Your use of the µTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In µTorrent, only files that you are explicitly

downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall µTorrent through the Add/Remove Programs control panel utility. In addition, you can control µTorrent in multiple ways through its user interface without affecting any files you have already downloaded."

13. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding."

14. Files or sets of files are shared on the BitTorrent network via the user of "Torrents." A "Torrent" is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to accomplish the download. This information includes things such as the name(s) of the file(s) being reference in the "Torrent" and "info hash" of the "Torrent." The "info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent." This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the

network who may be sharing part or all of the file(s) referenced in the "Torrent." "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing.

15. It should also be noted that the use of "Trackers" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

16. In order to locate "Torrent" files of interest and download the files that they describe, a typical user will user keyword searches on torrent indexing websites. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by "Torrent" files, only the "Torrent" files themselves. Once a "Torrent" file is located on the website that meets a user's keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process the "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file.

17. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), reference in the "Torrent," to include the remote peers/clients Internet Protocol (IP) addresses.

18. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search. The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent" file. Utilizing trackers and other BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) reference in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files.

19. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 hash value of that piece which is described in the "Torrent" file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

20. Law enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches the network. Law enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network reporting that they have been recently involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA-1 hash values of torrents. These torrents being searched for are those that have been previously identified by law enforcement as

being associated with such files. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

21. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer.

22. The investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many agencies are associated with the Internet Crimes against Children Task Force Program, to include Homeland Security Investigations. Many investigators involved in this effort are using the technology and methods described herein. This methodology has led to the issuance and execution of search warrants around the country resulting in numerous seizures of child pornography and arrests for possession, distribution, and receipt of child pornography.

THE INVESTIGATION

23. In January 2024, I was on a law enforcement portal which tracks the transmission/dissemination of child sexual abuse material (CSAM)[1] imagery across the Internet and/or P2P networks. The portal, which I had previously received training on how to access and query, is designed to show activity pertaining to P2P file sharing of CSAM files, in this case, on the BitTorrent Network. When I queried the portal, I identified an IP address 68.106.84.124 which was associated with numerous "files of interest" which the portal used as nomenclature for suspected CSAM.

24. Based on preliminary geolocating of IP address 68.106.84.124, the offender's physical location appeared to be somewhere around Roanoke, Virginia. I know from previous P2P investigations that the initial geolocation is an approximation, and the target premise would need to be identified through service of legal process on the IP address's Internet Service Provider (ISP). In this instance, the IP address 68.106.84.124, appeared to be Cox Communications, Inc.

25. By further analysis of the law enforcement portal, I identified the portal had logged investigative downloads of CSAM file(s) from the suspect's IP address. One investigator with whom I have worked previously, HSI Task Force Officer (TFO) M. Wells, had received direct connection download(s) from the target IP address. I contacted HSI TFO Wells, who independently checked his computer system and confirmed that he received the investigative downloads of CSAM from a target computer at the IP address 68.106.84.124. HSI TFO Wells provided the file(s) and associated digital logs for additional investigation.

[1] By accepted best practice, "child pornography" will hereinafter be referred to as "child sexual abuse material" or "CSAM."

26. On January 10, 2024, HSI TFO Wells was conducting an online investigation on the BitTorrent network for offenders sharing CSAM. An investigation was initiated for a device at IP address 68.106.84.124, because it was associated with a torrent that references 20 files, at least one of which was identified as being a file of investigative interest to CSAM investigations.

27. Using a computer running investigative BitTorrent software, a direct connection[2] was made to the device at IP address 68.106.84.124 (hereinafter "SUSPECT DEVICE"). The SUSPECT DEVICE reported it was using BitTorrent client software -UT360W- µTorrent 3.6.

28. On January 10, 2024, between 11:51 and 11:55 *[16:51-16:55 UTC]*, HSI TFO Wells' computer successfully downloaded 20 file(s) from the SUSPECT DEVICE with the following file names.

a. ! New ! (Pthc) Laura Swallows Cum.mpg

b. (Children-Sf-1Man) Pthc - Kylie Freeman Aka Vicky (11Yo) -Vicky Beginning And Swallows - [00.14.47].mpg

c. (G)1st-bj-KO 9yo_2013_specialRecode.avi

d. (~pthc center~)(opva)(July 2013) 8yo Thai Preteen Girl 1stBlowjob ••• 2013 (8mins)_x264.mp4

e. 2011 7yo niece - SUCK AND CUM IN MOUTH (sound 2013 byDRTMNDSK)).avi

[2] "Direct-Connection" refers to a software process wherein the law enforcement computer single-source downloads from the target device. Usually, P2P client software attempts to obtain pieces of the requested file(s) from as many sources possible in order to reassemble the requested file more quickly. By contrast, law enforcement P2P client software is designed to source the target file from a single target device; thus, the CSAM file had to have come from a computer device at the target IP address as described within.

f. 2011 7yo niece - SUCK AND CUM IN MOUTH (sound 2013 byDRTMNDSK)).avi_000060593.jpg

g. Linda (7Yo) Nov 2004 swallow cum ass gaping.mpg

h. PTHC - sucknew 7yo swallows daddys load (1min 6sec).avi

i. PTHC - sucknew 7yo swallows daddys load (1min6sec).avi_000043583.jpg

j. Suck&Swallow.avi

k. Veci 2009 (10yo Cum In Mouth Good).mpg

l. previews.rar

m. 1.jpg

n. 2.jpg

o. 3.jpg

p. 4.jpg

q. 5.jpg

r. 6.jpg

s. 7.jpg

t. 8.jpg

29. In reviewing the media files, I noted filenames contain descriptions indicative of child exploitation, including the ages of children (*7yo*[3]*, 8yo, 9yo, 10yo, 11yo*) and terminology known in the child exploitation community to be indicative of CSAM. These terms include "pthc," which is known to be an acronym for "pre-teen hardcore." Other indicative terminology

[3] The term "yo" as reference in the filenames is known to be an acronym for "year old."

includes references to *"children"* and *"Preteen."* I know that these are search terms for individuals attempting to locate CSAM imagery online or via peer-to-peer networks.

30. Additionally, I have conducted a visual review of the aforementioned CSAM media files. A summary/description of four (4) video media files are as follows:

a. **PTHC – sucknew 7yo swallows daddys load (1min 6sec).avi**

i. The video file is approximately 1 minute and 6 seconds in length. The video depicts what appears to be a nude prepubescent female engaged in fellatio with an adult male's erect penis. Later in the video, the adult male appears to grab/hold the prepubescent female's hair and with the female's mouth open, the adult male appears to ejaculate into the female's mouth.

b. **(~pthc center~)(opva)(July 2013) 8yo Thai Preteen Girl 1stBlowjob ••• 2013 (8mins)_x264.mp4**

i. The video file is approximately 7 minutes and 49 seconds in length. The video depicts what appears to be a prepubescent female clothed in a red dress/outfit engaged in fellatio with an adult male's erect penis. Throughout the video, the prepubescent female is engaged in fellatio with the adult male in multiple different positions, including but not limited to sitting, kneeling, and standing. Later in the video, the prepubescent female, with the dress/outfit separated exposing her breast, is observed laying down on what appears to be a piece of furniture. The adult male is then observed straddling/kneeling over the prepubescent female's chest. Fellatio is continued until the adult male ejaculates into the mouth of the prepubescent female.

c. **Suck&Swallow.avi**

i. The video file is approximately 10 minutes and 13 seconds in length. The video depicts what appears to be a clothed prepubescent female wearing sunglasses. As the video progresses, the prepubescent female is observed removing her clothing prior to engaging in fellatio with an adult male's erect penis.

d. **2011 7yo niece - SUCK AND CUM IN MOUTH (sound 2013 byDRTMNDSK)).avi**

i. The video file is approximately 1 minute and 9 seconds in length. The video depicts what appears to be clothed prepubescent female engaged in fellatio with an adult male's erect penis.

31. In addition, HSI TFO Wells served an Albemarle County Commonwealth Attorney's[4] Administrative Subpoena on Cox Communications, Inc., pertaining to the IP address 68.106.84.124, port # 62557[5], for the date and time associated with the aforementioned downloads.

32. Cox Communications, Inc., provided information regarding IP address 68.106.84.124, port # 62557, including the following subscriber name and physical address. Cox Communications also provided an email address and telephone number.

a. Joshua Jennings

b. APT 6 2114 WINDSOR AVE SW ROANOKE, VA 24015

[4] HSI TFO Wells is also a Detective with the Albemarle County Police Department.

[5] A port number is an extension of an IP address and identifies a process for an Internet or other network traffic to be forwarded upon arriving at a server.

33. Upon receiving the aforementioned information, I performed open-source and law enforcement database queries. I identified driver's license information for JENNINGS from the Virginia Department of Motor Vehicles (DMV). The information showed an address of 2114 WINDSOR AVE SW APT 6, ROANOKE, VA 24015.

34. Further, JENNINGS was identified as a "Sexually Violent Predator" and currently registered on the Virginia State Police (VSP) Sex Offender and Crimes against Minors Registry. JENNINGS has multiple Virginia felony convictions, including (1) possession of obscene material with a minor; (2) production, distribution, or financing of child pornography; and (3) possession of a weapon/ammunition by felon (not firearm). His criminal history also shows numerous felony probation violations. Both databases indicate that JENNINGS' address is 2114 WINDSOR AVE SW APT 6, ROANOKE,VA 24015. Upon review of the VSP Sex Offender Registry, the following information was identified.

a. Registration Number: 20218

b. Status: Active

c. Tier: Tier 1[6]

d. Reg. Renewed: 01/10/2024

e. Initial Registration: 11/09/2006

35. In February 2024, I spoke with Postal Inspector S. McCafferty of the United States Postal Inspection Service (USPIS). USPIS Postal Inspector McCafferty confirmed an individual using the name Joshua JENNINGS had received parcels at the SUBJECT PREMISES.

[6] According to VSP Trooper D. Lockliear, the VSP Sex Offender and Crimes against Minors Registry is incorrect, and JENNINGS is actually listed as a Tier III Offender, meaning a lifetime sex offender status.

36. Upon conducting surveillance and additional database queries, a vehicle was identified as being registered to JENNINGS, a blue/grey Jeep (VA: TVD-4223). Further research with the Department of Motor Vehicles identified the following information:

a. Joshua Lee JENNINGS

b. 2114 WINDSOR AVE SW APT 6, ROANOKE VA 24015

c. VIN: 1C4NJCBA2ED881780

37. To date, my surveillance and information indicates that the SUBJECT PERSON resides at the SUBJECT PREMISES alone.

38. In February 2024, I spoke with Commonwealth of Virginia Probation and Parole Officer L. Edwards, who advised the SUBJECT PERSON is on active probation. As such, the SUBJECT PERSON is only authorized to have an Android cellphone and a PlayStation 5, with limitations. Further, the Android cellphone has monitoring software installed. Thus, the SUBJECT PERSON may be more likely to conceal additional electronic devices and storage media.

39. Although it is possible that µTorrent or a similar software client could be used on an Android cellphone or a Playstation 5, this would be atypical, and would require a fairly high degree of technical sophistication. In my training and experience, µTorrent and similar programs are ordinarily used on desktop or laptop computers, not on phones or on gaming consoles. Given this fact, and the fact that the SUBJECT PERSON's phone is monitored, I believe that the SUBJECT PERSON likely possesses other unauthorized electronic devices and/or storage media.

40. Collectors of CSAM also frequently possess their collections on cellular phones. CSAM is easily transferable in that it normally consists of computer files, such as video files or

images. These types of media can easily be transferred from computers to cell phones via, among other methods, cloud storage platforms. In my training and experience, many people carry their phones on their persons everywhere they go. Given the ubiquity of cell phones, I submit that there is probable cause to search the person of JENNINGS, along with any containers such as bags or boxes within his immediate control that may reasonably contain the information further described in Attachment B. Because of the small size and portability of electronic devices, as well as electronic storage media, such as thumb drives, vehicles belonging to or operated by JENNINGS may also be a storage location for evidence. More specifically, the SUBJECT VEHICLE is likely to contain evidence, whether it is found on the SUBJECT PREMISES or not.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

41. I submit that if an electronic device(s) is found at the SUBJECT PREMISES, on the SUBJECT PERSON, or in the SUBJECT VEHICLE, there is probable cause to believe that contraband or CSAM evidence will be stored on the device(s), for at least the following reasons.

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear, rather that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

42. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device(s) because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual

memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the data files were created and the sequence in which they were created.

b. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and duration, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer

accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information descried herein may either inculpate or exculpate the computer user. Finally, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always something easily reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

43. I know that when an individual uses an electronic device to obtain CSAM or child abuse materials over the internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used, data that was sent or received, and other records that indicate the nature of the offense.

44. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

45. *Biometrics*. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search or seizure pursuant to this warrant. I seek this authority based on the following:

a. In my training and experience, it is likely the SUBJECT PREMISES, the SUBJECT PERSON, and the SUBJECT VEHICLE will contain at least one cellphone or tablet due to the ubiquitous use and ownership of these electronic devices generally.

b. I know from training and experience, as well as from information found in publicly available materials including those published by cellphone manufacturers, such as Apple, that some models of electronic devices, such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") or use facial recognition software in lieu of or in combination with a numeric or alphanumeric passcode or password.

c. If a user enables this fingerprint or facial recognition coding on a given electronic device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. Facial recognition software works by allowing the user to hold the electronic device at a certain angle to their face to unlock the device. In my training and experience, users of devices that offer these tools often enable them because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a

more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device(s).

d. In some circumstances, a fingerprint or face cannot be used to unlock a device, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device via Touch ID or facial recognition software exists only for a short time. Touch ID also will not work under other circumstances.

e. The passcode or password that would unlock the electronic device(s) found during the search of the SUBJECT PREMISES, the SUBJECT PERSON, or the SUBJECT VEHICLE is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) or use the user's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via Touch ID or with facial recognition software with the use of the fingerprints or facial image of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

f. In my training and experience, the person who is in possession of a device(s) or has the device(s) among his or her belongings at the time the device(s) is found is likely a user of the device. However, in my training and experience, that person may not

be the only user who can unlock the device, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require the SUBJECT PERSON and any occupant of the SUBJECT PREMISES or the SUBJECT VEHICLE to press their finger(s) against the Touch ID sensor of the locked device(s) or hold the device up to their face found during the search of the SUBJECT PREMISES, the SUBJECT PERSON, and the SUBJECT VEHICLE in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID or facial recognition software.

g. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a cellphone via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s) found in the SUBJECT PREMISES, the SUBJECT PERSON, and the SUBJECT VEHICLE as described above within the five attempts permitted by Touch ID or facial registration software, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would

permit law enforcement personnel to obtain from any person whose device is to be searched any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices, including to (1) press or swipe the fingers, including thumbs, of those persons to the fingerprint scanner of the devices found at the SUBJECT PREMISES, SUBJECT PERSON, and SUBJECT VEHICLE; (2) hold the devices found at the SUBJECT PREMISES, SUBJECT PERSON, and SUBJECT VEHICLE in front of the face of those persons to activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES, SUBJECT PERSON, and SUBJECT VEHICLE in front of the face of those persons to activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

i. The proposed warrant does not authorize law enforcement to require that the persons whose device is to be searched state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel those persons to state or otherwise provide that information. However, the voluntary disclosure of such information of such information by those persons would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of those persons for the password to any devices, or to identify which biometric characteristic (including the unique finger(s)

or other physical features) unlocks any devices, the agents will not state or otherwise imply that the warrant requires the person to provide such information and will make clear that providing such information is voluntary and that the person is free to refuse the request.

CONCLUSION

46. I submit that there is probable cause to believe that the SUBJECT PREMESIS, the SUBJECT VEHICLE, and the SUBJECT PERSON (including any closely associated containers), will contain contraband, along with evidence and instrumentalities of violations of 18 U.S.C. § 2252. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, SUBJECT PERSON, SUBJECT VEHICLE, as more particularly described in Attachment A-1, A-2, and A-3, authorizing the seizure of the items described in Attachment B.

Respectfully submitted,

BRANDON M SMOCK Digitally signed by BRANDON M SMOCK Date: 2024.02.22 21:57:52 -05'00'

Brandon Smock, Special Agent
Homeland Security Investigations

Subscribed and sworn to me by telephone this 23rd day of February, 2024.

Hon. C. Kailani Memmer
UNITED STATES MAGISTRATE JUDGE